Cover Page

U.S. Department of Energy Office of Science
Scientific Discovery through Advanced Computation Solicitation LAB01-06
National Collaboratories and High Performance Networks

Distributed Security Architectures

Middleware for Distributed Computing

For the period July 1, 2001 – June 31, 2004

Principal Investigator

Name	**Mary Thompson**
Institution:	Lawrence Berkeley National Laboratory
Tel:	(510) 486-7408
Fax:	(510) 486-6363
Email:	MRThompson@lbl.gov

Co-Investigators

Name:	**Srilekha Mudumbai**
Institution:	Lawrence Berkeley National Laboratory
Tel:	(510) 486-6297
Fax:	(510) 486-6363
Email:	SSMudumbai@lbl.gov

Name:	**Abdelilah Essiari**
Institution:	Lawrence Berkeley National Laboratory
Tel:	(510) 495-2872
Fax:	(510) 486-6363
Email:	AEssiari@lbl.gov

Table of Contents

Abstract

The overall goal of this project is to provide assured, policy-based access control for computer mediated resources such as data archives and instrument systems, that operate in wide area network environments; grid services such as network monitoring, computing resources and bandwidth reservation; and potentially fine-grained, object method level access control (such as might be used to implement "need to know" restrictions on databases).

We propose to continue investigating and implementing practical solutions to the security needs of distributed systems based on the emerging PKI standards and implementations. In particular, to provide a modular authorization service that compares a requestor's authenticated X.509 identity certificate with a set of signed policy documents describing the access policy for the requested resource. These policy documents are created and maintained by stakeholders for the resource, independent of the resource server platform.

In addition future work will focus on integrating our authorization mechanism with the core of emerging standards such as the IETF's Transport Layer Security (TLS), WebDAV protocols, Generic Authentication and Authorization interface (GAA) and the Grid Security Interface (GSI). We plan to integrate with a monitoring agent system and to provide access control for secure multicast groups. Both of these uses of Akenti require changes to the types of policies that it can support. In order to facilitate Akenti's use by new and continuing applications the basic policy engine will be made more robust and the interfaces will be expanded.

1 Narrative

1.1 Motivation

DOE scientific resources - instruments, data, and collaborations - that are accessed via open networks or as part of the DOE Science Grid require protection against unauthorized use. We have now had several years of experience with collaboratory environments where the resource stakeholders come from administrative domains that are separate from where their resources are kept. This experience has emphasized the importance of having uniform cross-domain standards and procedures for setting and enforcing policy on resources. The current practice of needing a privileged account on each resource machine in order to login and edit specific access control files on each machine does not scale to the number of machines and stakeholders that will participate in the next generation of collaboratories and grids.

Another requirement of Grid and collaboratory environments is the need for a user to delegate his access rights to processes that are running on his behalf. This need typically arises when a job that is executing on behalf of a user needs access to data or additional compute resources that are only available to the user. The program needs to present a proxy credential that securely identifies it as operating on behalf of the user. Current state of the art, supports unrestricted delegation in certain contexts, but the need for more restricted delegation and broader recognition of proxy certificates is clear.

We have built a research prototype implementing a multiple stakeholder use condition – user attribute model of authentication. Called Akenti, it provides a flexible, easily managed mechanism, which strongly controls access to distributed resources, by widely distributed users. Akenti is an authorization system designed to address the issues raised in allowing restricted access to distributed resources which are controlled by multiple stakeholders from different administrative domains. The stakeholders are the people with authority to grant access to resources and may be both physically and organizationally remote from the resource. Akenti makes access control decisions based on one set of digitally signed documents that represent the authorization instructions and another set that represent user attributes. Existing public-key infrastructure and secure message protocols provide confidentiality, message integrity, and user identity authentication, during and after the access decision process. Akenti enables stakeholders to remotely and securely create and distribute instructions authorizing access to their resources. This is in contrast to most access control systems in use today, which assume that access policy is contained in a centralized server (such as DCE) or a protected file located on the machine that controls access to the resource. This centralized access policy is inconvenient for multiple, remotely located stakeholders.

Our experience using Akenti within the Diesel Combustion Collaboratory [12] and with other applications emphasizes several lessons and suggests some needed enhancements to the current authentication and authorization implementations. One lesson is that a major challenge in designing usable access control mechanisms is to balance the richness and extensibility of the features with the comprehensibility of the resulting access policies. If there is insufficient flexibility as to what can be expressed the stakeholder is unable to set his desired policy. If on the other hand there are too many features, he may set a policy and not understand clearly what access is allowed to what users. This motivates more research into policy languages including the ability to handle multiple policy languages, to clearly provide for role-based models of authorization and to allow for more dynamic polices. It is our belief that the best approach to the usability of rich policy languages is to provide the stakeholders with a wide variety of tools to set and test authorization policy. We found that while distributed storage of use condition and attribute certificates was a goal of our prototype, it was also necessary to provide ways of storing user generated certificates on the resource server to accommodate stakeholders who do not have a secure Web-accessible place to store certificates.

Another lesson learned is the importance of standardizing proxy certificates to allow processes to run with a user's credentials. This motivates the implementation of a new TLS record protocol [11] to create such certificates, changes to the path validation algorithms to verify chains of proxy certificates and to return the initiator's identity and extending the Akenti authorization mechanism to understand proxy certificates.

New developments in distributed computing tools need to be accommodated by our authentication and authorization framework. One such standard that is gaining popularity in the collaboratory community is WebDAV [8], which is a set of extensions to HTTP to allow for distributed authoring of information. We plan to investigate extending the Akenti policy analyzer to understand the access control entries that are created and used by the WebDAV Access Control protocol. It will also be necessary to have an implementation of WebDAV that uses X.509 identity and proxy certificates for user authorization.

1.2 Background

Access control is a means for enforcing an authorization policy. In a client-server architecture, the clients (on behalf of users) attempt to access resources that are controlled by servers. A priori authorization decisions govern which users may access which servers for what purposes and under what conditions. These decisions are reflected in an access control policy. Users must be identifiable in a way that can be matched with access control policy. In traditional centralized a user is identified by a system centered user ids such as Unix userid or Kerberos identities. The current collaboratories and grids have chosen to use X.509 identity certificates for user identification and TLS to authenticate the presenter of a X.509 certificates. Once a user has been authenticated, he may be mapped on to a local userid as in Globus [7], or his X.509 distinguished name may be used directly in access control information as in Akenti [14].

Over the last three years an Akenti prototype has been developed and deployed in many applications and several testbed environments. It is used in the Diesel Combustion Collaboratory (http://www-collab.ca.sandia.gov/Diesel/ui/security.shtml) to allow restricted Web access to several kinds of information. It has been used locally at LBNL to allow restricted access to download the Akenti code (http://www.itg.lbl.gov/Akenti/downoad.html) and to allow protected file uploads and being used as part of the Distributed Collaboratories Toolkit (http://www-itg.lbl.gov/Collaboratories/) to protect access to some instruments and monitoring programs.

?? Akenti has been integrated with several standard server / gateway mechanisms

- We have developed an Akenti enhanced Apache Web server that uses the SSLeay patches (http://www.apache-ssl.org) to Apache to get the client ID certificate. We have replaced the Apache standard access control module with one that calls Akenti, thus replacing the standard Web user and password access control with one implemented by Akenti and based on the ID certificate the user passed in, and the distributed use condition certificates that have been created by the stakeholders for the documents.
- A pilot integration of Akenti with a CORBA ORB using the Object Management Group (OMG) defined interceptor mechanism has been built. Using the SSL-enabled version of Iona's Orbix (http://www.iona.com), the identity of the client and the name of the CORBA object that is being invoked can be passed to Akenti at the time the invocation is attempted. Akenti uses this information, along with an authority file for the objects and whatever use conditions exist for the object to allow or deny access to an object. Access can be controlled on the object name, and, optionally, on the object and method being invoked. This same approach has been applied to the DCC PRE environment, which is based on CORBA functions.
- A prototype implementation of a secure group communication has been started. The CLIQUES [1] group key agreement algorithm has been combined with Akenti access control to allow only authorized members to join a communication group.

?? Akenti integration with applications

- A secure Akenti–enabled Web server is being used at LBNL to control distribution of the Akenti code, to allow restricted file uploads and to secure a prototype Image Library (https:// imglib.lbl.gov). In these applications, the Web server uses Akenti to grant access to existing files and the scripts that are used to create new files. Then the scripts call Akenti directly to check on fine-grained access before modifying the data on the server.
- Akenti is being used by the Diesel Combustion Collaboratory (DCC) via the Akenti-Web server to control access to the ORNL electronic notebook and to the Data Archive. In each case an Akenti-enabled Web server does the initial access control to a script and then the script calls Akenti for fine-grained access control including searching, reading and modifying of the protected data.
- We have integrated Akenti access control with a PRE server. PRE is Sandia's remote server protocol that is used extensively by the DCC for providing modeling servers to the Collaboratory members. PRE is implemented using CORBA which provides call-outs at appropriate places in the connection process to check for access permissions. Using an advanced version of PRE that is implemented over an SSL-enhanced version of CORBA, we instrumented these call-outs to use Akenti access control.

- Akenti access control is available as part of a remote camera controller deployed by the Distributed Collaboratories Toolkit where it is used to determine what users may take control of a remote camera. The connection between the client and the server was changed to be an SSL connection that presented and verified the client's identity. This identity is then used by Akenti to check the client's access to the software that control actions on a camera located at the server machine. The two sides of the camera controller software then negotiate a shared key that is used by the subsequent UDP command message to verify the identity of the sender. See (http://www.itg.lbl.gov/Akenti/sc98/akenti_apps.pdf) for more details.
- Preliminary work has been done to integrate Akenti into a network test suite (lblnettest) being developed by the Advanced Visualization Communication Toolkit project at LBNL. The suite allows coordinated use of multiple existing network testing utilities (e.g. ping or NLANR's iperf), to achieve an overview of network conditions. It is run as a server which is accessible to clients on remote machines. Since some of the tests supported can use considerable resources on the test machine and cause network congestion, access to the server must be controlled. An SSL connection is used to securely establish the identity of the client to the lblnettest server. This identity is passed to Akenti to determine the access rights of the requester; which are then used by lblnettest to determine what, if any, tests the client is authorized to run.

?? Usability issues

- We have dealt with the problems of debugging the policy and use conditions and educating the users and stakeholders by providing several methods for the remote user to monitor what the Akenti server is doing. We have written an applet that talks to the logging monitor on the secure resource machine and provides a real-time graphical display of the steps taken to check a user's access to a secure resource. (http://imglib.lbl.gov/StartMonApplet.html). We have provided a Web interface that will display the policy imposed by stakeholders on resources. Both of these facilities are available to anyone who has basic access to the resource tree. They do not need to have access to the specific resource they are querying. In a thoroughly debugged setup, these functions might be viewed as a security hole and disabled. But when a system is being set up and stakeholders are learning how to set up use conditions, they have proven extremely useful.
- The graphical user programs to generate UseCondition and Attribute certificates have been substantially redesigned as a result of user feedback. The new versions step a user through the process of certificate generation, providing menus of allowable values, and checking for inconsistent input. The new implementation is more modular, uses the newer Java Swing classes and has eliminated dependencies on Solaris native cryptographic libraries. In response to user feedback, these versions allow the uploading of the certificates to the resource servers, to accommodate users who do not have a secure Web-accessible site of their own in which to place the certificates.

?? Code release and examples

- Akenti 1.0beta is ready for release to "friendly" users (those who understand a bit about PKI and will provide feedback) (http://www.itg.lbl.gov/Akenti/download.html)
- Secure Apache Web server integrated with Akenti (to provide directory- and object-level access control) is ready for first beta release
- An example secure Orbix CORBA ORB - Akenti integration is available (Akenti enforces use conditions on ORB methods and objects)
- Documentation is available: user (http://www-itg.lbl.gov/Akenti/docs/user_guide.html), stakeholder (http://www-itg.lbl.gov/Akenti/docs/stakeholder.html), and administration (http://www-itg.lbl.gov/Akenti/docs/admin.html).

1.3 Research Design and Methods

1.3.1 Specific goals for authorization and authentication

The fundamental goal of the Akenti authorization system is to provide assured, multiple stakeholder control over distributed resources accessed by physically and administratively distributed users. This goal in turn requires distributed management of all information needed for access decisions. To achieve this end we use X.509 identity certificates generated and managed by multiple institutions to identify users; we use trusted third-party certification of user attributes; and we build on existing protocols for cross domain authentication such as TLS and GSI. If the Akenti authorization system is going to be useful to the community, it must meet the following goals:

- ?? Be easily integrated with applications including those that require a light-weight authorization mechanism such as agent systems and secure group applications; Continue to support other DOE grid and collaboratory research environments and middleware.
- ?? Provide a rich policy language and set of authorization models that allow collection, object and action levels of authorization;
- ?? Present an easy to use interface for stakeholders to set and evaluate policy;
- ?? Be capable of supporting emerging approaches like GAA [13], GSI [2], the newly designed delegation certificates [15,16], WebDAV [3,8] and XML policy certificates;

Our experience with using Akenti authorization in a collaboratory environment and with a variety of applications has demonstrated the validity of our goals and reinforced the requirement for simple interfaces for both applications and stakeholders.

1.3.2 Approach

Akenti provides the functions an independent certificate analyzer that locates and verifies all of the information necessary to determine stakeholder use conditions and user attributes that satisfy those use conditions (http://www.itg.lbl.gov/Akenti).

All information required to make an authorization decision is encoded in digitally signed documents that can be generated and managed in the trust domain of the stakeholders (http://www.itg.lbl.gov/Akenti/docs/specs.html#PolicyModelOverview).

The Akenti analyzer will understand the proxy/delegation certificates generated by GSI to allow resources to be used by a third party acting as a proxy for a user. It will also recognize the restricted delegation extensions that may carry delegation tracing or rights restriction information.

The resource gateway will use Akenti as an authorization service e.g., something that makes access control decisions about a resource. We assume that the client connection to application server / security gateway is by a secure protocol (e.g., TLS), which authenticates the user and passes the client /user credentials to the gateway server. These credentials may be end-entity identity certificates or delegation certificates. The gateway server in turn passes the identity of the user and the resource to Akenti. Akenti is able to find the root policy certificate for the resource from the resource name.

Akenti then locates and validates all stakeholder use conditions; locates and verifies user attributes (that will satisfy the use conditions); and then returns the allowed actions of this stakeholder on this resource. (If no actions are allowed the secure connection fails to complete.) If the resource is subject to run-time constraints that the resource gateway must monitor (such as limited resource allocation), the allowed actions are passed back with constraints that must be verified and enforced by the resource gateway.

We are also intending to implement a GAA interface to Akenti. The GAA approach passes the entire policy back to the caller for possible modification, and then accepts a policy and a user credential and does the analysis for what rights are granted. Another slightly modified interface will hand back a short-term capability certificate, signed by the Akenti server, that would specify a resource name, user name and allowed rights. The user could then produce that capability, along with his authenticated identity and be granted immediate access to a resource. Another possibility to be investigated is using these capability certificates as the restricted rights extension of an impersonation certificate.

Our experience with using Akenti authorization in a collaboratory environment and with a variety of applications has shown the need to integrate the authorization mechanism with the ability of a user to delegate all or some rights to a proxy. GSI has provided a prototype for unrestricted delegation credentials within a Globus environment. We plan to implement the proposed TLS protocol to create the proposed IETF impersonation certificates and to continue to work to establish standards for delegation tracing and rights restrictions extensions in impersonation certificates.

1.3.3 Proposed Work

1.3.3.1 Support ease of use by applications and support for ongoing grid and collaboratory projects

- **Standalone server:** Investigate the issues, design, and implement Akenti as a secure, stand-alone access control service. Akenti currently is implemented as a library module which applications access via local procedure calls. The first stand-alone version will implement a simple message protocol over openSSL and initially be used by the Reliable and Secure Group communication prototype being developed at LBNL [1]. We will investigate allowing resource servers to upload their initial policy information via secure connections (following authentication and access control to prevent use by unauthorized servers) in order to let one Akenti server support several different resource servers. This policy upload will be used in the implementation of the GAA interface. The API for the standalone server will include an interface to flush the cached certificates.
- **Changes to Akenti policy engine**: Many of the changes specified in the following sections were motivated by the needs of particular application domains. For example the SciDAC National Collaboratory to Advance the Science of High Temperature Plasma Physics for Magnetic Fusion foresees a need to base authorization decisions on a combination of static policy and current unused quota for computational resources. This will require changes to the Akenti API to either make callouts to find out about current quota values, or to return conditional access rights. The SciDAC Reliable and Secure Group Communication proposal requires a way to pre-determine a user's right to join a group, which has motivated the creation of capability certificates. As that project builds a prototype, Akenti will need to provide these capability certificates and may need to provide methods for supporting more dynamic policies for group authorization. The SciDAC Self Configuring Network Monitor proposal may also use an Akenti generated capability certificate to get permission to start the monitoring process. As in the Reliable and Secure Group Communication proposal there is a need to do the heavy weight authorization before asking the service for access. The signed capability certificate is a way to let the user do the authorization in advance and leave the resource gateway with the simple task of verifying the capability signature and interpreting the rights contained in it. The Access Grid has also expressed an interest in using Akenti to authorize access to shared conferencing and visualizations. The policies here may be relatively dynamic, similar to those required by the Group Communication prototype. As the DOE Grid expands, it will require more dynamic and more scalable authorization policy than the single Globus CA-signing policy and Grid map file [6]. We intend to see if the Akenti policy approach can be used there. In order to facilitate these anticipated extensions to the Akenti policy engine, we have redone the original design of the Akenti policy engine to be object-oriented and extensible. This design has produced a more robust version of Akenti that will facilitate its use in a wider variety of applications.

1.3.3.2 Support rich policy languages and authorization models

- **Address different policy representations** e.g., token based as in the current GAA implementation or certificates expressed in XML. Investigate what sort of policy could support both the WebDAV access control language and the Akenti trust model. Implement policy collection and analyzer plug-ins to support different policy languages.
- **Provide support for dynamic policies**. Investigate the issues related to permissions that require semantic understanding by the policy engine such as time-of-day and resource use limits. Define and implement policy extensions that support the runtime constraints on UseCondtions and attributes.
- **Issue capability certificates**. In order to support applications that need to separate the heavy-weight Akenti distributed policy authorization process from a possibly frequent and quick authorization, have the Akenti policy engine return a signed capability certificate as an alternative to a rights string. This capability

certificate can then be used to grant the bearer rights to a resource if the gateway recognizes Akenti as a trusted third party.

1.3.3.3 Support easy to use stakeholder interfaces to set and test policy

?? **Develop an graphical interface to create policy certificates**. Develop an interface similar to the ones used to create use condition and attribute certificates for the policy certificates asssociated with each protected resource. Currrently this per-resource level root information is contained in local files on the resource server. In order to complete our goal of having all stakeholder functions provided via remote and easy to use interfaces, this information will be contained in a signed certifcate which can be created via calls to the resource definition server.

1.3.3.4 Support emerging standards

?? **Changes to Akenti policy engine**. Investigate the issues and then implement a prototype of the new IETF Certification Revocation List standards [10]. Extend the API to include the GAA policy interface. Investigate integrating top level Akenti policy statements with WebDAV controlled resource namespaces.

?? **Implement a new TLS record protocol to create the proposed proxy certificates**. Extensions to IETF standards to support X.509 Proxy Certificates are being pursued at the IETF meetings. The proposed proxy certificate profile is a cleaned up version of the proxy certificates implemented by GSI. The TLS extension formalizes a protocol for the creation of such certificates. We plan to collaborate with the work at ANL in extending GSI to support this new format for proxy certificates and to extend Akenti to use the proxy certificates for authorization.

?? **Restricted delegation in proxy certificates**. A limited delegation certificate that allows a user to delegate some privileges to the holder of the certificate is needed in distributed applications where a resource is to be accessed by a third party operating on behalf of a remote user. For example, in the Diesel Collaboratory, a modeling server run on behalf of a user may want to store output data to that user's data archive. The current proposed X.509 proxy certificate defines two types of restriction fields. One traces the parties involved in the delegation and the other adds an explicit restriction of the rights allowed to the bearer of the delegated certificate. We will continue to work on refining and generalizing these extensions with a goal of presenting them to IETF. We plan to either adapt GSI or the applications and servers that use GSI, to implement the restricted rights field. We will also adapt the Akenti authorization scheme to recognize the rights restrictions, so that in addition to determining the rights of the originator of the delegated credential, those rights will be further restricted by any rights restrictions found in the chain of delegated certificates. Use conditions may need to include the right to delegate permissions.

?? **GSI:** Investigate the issues, design and implement an integration of Akenti into the Grid Security Interface. Investigate how Akenti policy certificates can be used to replace the Globus map files in situations where the access to resources needs to be controlled by remote Grid stakeholders rather than local host policies. Support an Akenti Attribute Certificate that maps a user DN to a local userid for a specific domain. Extend the Akenti policy engine to recognize Grid proxy identity certificates.

?? **WebDAV**: We will investigate the integration of Akenti authorization policy with the WebDAV authorization mechanism. WebDAV (Web-based Distributed Authoring and Versioning) is an IETF standard set of extensions [8] to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. As such it is a useful collaboration tool that both the Cosmology Collaboratory Pilot and the Multi-Scale Chemical Science Collaboratory are intending to use to facilitate information sharing. WebDAV implementations currently use the standard Web .htaccess files that restrict access to locally defined userids and passwords. There is a proposed protocol for setting and querying access control entries in HTTP [3]. Newer versions of the SSL-Apache Web server also allows access control based on components of a user identity certificates but provide no mechanisms to define the trusted CAs, and stakeholders. Since the two collaboratories mentioned above are also going to be using GSI for authentication and Akenti for authorization it would be very useful to be able to use the x.509 identity and proxy certificates to gain access to WebDAV controlled resources. Providing a common interface to setting and querying access policy between Akenti and WebDAV would likewise simplify life for the stakeholders of the collaboratories. One approach is to replace all the access information with Akenti policy certificates as we have done with earlier versions of the Apache Web servers and then provide an WebDAV interface for

querying the policy. Another approach to be investigated is to only replace the top level policy which defines the trusted CAs and stakeholders with Akenti policy certificates and leave the lower levels as unsigned files on the server machine which can be updated via the HTTP extensions. The Akenti policy engine could deal with the additional policy format by using a plug-in policy analyzer that understands the format.

1.3.4 Tasks and Milestones

1.3.4.1 First year milestones

1.1 Version 1.1 of the Akenti policy engine will be thoroughly tested and deployed to as part of a secure Apache server to control access to Web controlled resources such as file upload scripts, Portal Grid access and document pages that should only be read by Grid members.

1.2 The Akenti policy engine will be deployed as a stand-alone server to provide capability certificates to the Reliable and Secure Group Protocol prototype. It will provide an interface to allow a stakeholder to flush any revoked certificates from its cache.

1.3 A graphic interface will be provided to create policy certificates similar the ones used to create use condition and attribute certificates.

1.4 A specification for restricted proxy credentials is being drafted at GridForum and IETF. We have specified an Akenti policy language version of the proxyRestriction field and will begin implementing it within the GSI API..

1.5 Begin implementation of the TLS protocol for creating a proxy certificate.

1.3.4.2 Second year milestones

2.1 Akenti will be integrated with GSI as an optional replacement for the Globus Map File. Non-legacy applications that control access to resources and are accessed via GSI will have a simple API they can call to determine the permissions of the user represented in the GSS context that they hold

2.2 Further definition of the Akenti policy language proxyRestriction willl be done and the first implementation finished.

2.3 Implementation of the TLS proxy delegation protocol that handles the trace delegation and restricted rights will be completed.

2.4 Add the ability to handle CRLs to the Akenti policy engine. Follow the OCSP as an alternative to CRLs.

2.5 Further investigation of the usefulness of XML certificates and other possible policy languages will be undertaken.

2.6 The merits of replacing Akenti attribute certificates with attribute certificates as defined in the PKIX working draft on attribute certificates [5] will be considered and may be implemented if there is sufficient advantage to using as standard certificate form.

1.3.4.3 Third year milestones

3.1 Support for additional dynamic and conditional policies as required by grid and collaboratory applications will be provided.

3.2 Actions will be taken to follow up on IETF acceptance of restricted rights extension to proxy certificates.

3.3 Continuing support for Grid and Collaboratory projects authorization needs will be provided such as dynamic grroup policies, and integration with WebDAV will be provided.

1.4 Connections to other projects

Akenti has provided policy based access control for the Diesel Combustion Collaboratory and we intend to continue to co-operate with the successor Multi-Scale Chemical Science Collaboratory proposed by the DCC team at Sandia and PNNL.

Akenti has been used in the CORBA based PRE modeling servers of the DCC and is included in a SBIR phase 1 proposal called CoDeveloper to implement the CORBA authorization call-out. The secure versions of CORBA ORBS are implemented over TLS and use X.509 identity certificates to authenticate users. The ORB also provides call-out hooks at points such as launching server or executing a method call. These call-outs are an easy point at which to insert calls to the Akenti check_access interface.

Integrating Akenti with GSI is part of the SciDAC National Collaboratory to Advance the Science of High Temperature Plasma Physics for Magnetic Fusion proposal to provide X.509 identity based authentication and policy based authorization for remote job authorization, MDSplus access and MSSQLServer access. The integration of Akenti and GSI is also a requirement of the SciDAC DOE Science Grid proposal [4] .

We are working with the Reliable and Secure Group Communication project at LBNL to provide authorization for members to join a secure communication group. This work is the motivation for the standalone Akenti server interface and for Akenti to provide short lived capability certificates. The secure group protocol wants to establish access before the group joining protocol is started, in order to make the join protocol which involves all the members of a group proceed faster.

2 Literature Cited

1. Agarwal, D., Chevassut, O., and Tsudik, G., "Integrating Access Control with Secure Group Communication for Wide-Area Networks", Tech Report LBNL-46652, Lawrence Berkeley National Laboratory, August 2000.
2. Butler, R., Engert, D., Foster, I., Kesselman, C., Tuecke, S., Volmer, J., Welch, V., "A National-Scale Authentication Infrastructure". IEEE Computer, 33(12):60-66, 2000.
3. Clemm, G., Hopkins, A., Sedlar, E., Whitehead, J. "WebDAV Access Control Protocol", draft-ietf-webdav-acl-04.txt
4. DOE Science Grid , http://www-itg.lbl.gov/Grid/
5. Farrell, S., Housely, R. "An Internet Attribute Certificate Profile for Authorization", draft-ietf-pkix-ac509prof-06.txt
6. Foster, I., Kesselman, C., Tsudik, G., and Tuecke, S., "A Security Architecture for Computational Grids", Proceedings of the 5th ACM Conference on Computer and Communications Security, 1998.
7. Foster, I., Kesselman, C., and Tuecke, S., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International Journal of Supercomputer Applications, 2001.
8. Goland, Y.,Whitehead, E., Faizi, A., Carter, S., Jensen, D., " HTTP Extensions for Distributed Authoring -- WEBDAV", IETF RFC2518
9. Hoo, G., Jackson, K., Johnston, W., "Design of the STARS Network QoS Reservation System" Journal of Communications and Networking (JCN) - special issue on QoS in IP networks (June 2000).
10. Housley, R., Ford, W., Polk,W., and Solo,D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 2459, Draft Update draft-ietf-pkik-new-part1-06.txt, January 1999.
11. Jackson, K., Tuecke, S., and Engert, D., "TLS Delegation Protocol," Internet Draft draft-ggf-tls-delegation-05.txt, 2001, http://www.gridforum.org/security/ggf1-2001-03/draft-ggf-x509-res-delegation-01.pdf
12. Pancerella,C., Rahn, L., Yang, C., " The Diesel Combustion Collaboratory: Combustion Researchers Collaborating over the Internet", Proceedings of ACM/IEEE SC99 Conference, November 13-19, 1999, Portland, Oregon, USA _ (this is not actually referenced. I had in mind the lesson that credential delegation was required in any system of distributed computation and data access.)
13. Ryutov, T., Neuman, C. "Access Control Framework for Distributed Applications" IETF Internet-draft draft-ietf-cat-acc-cntrl-frmw-05.txt November 22, 2000
14. Thompson, M., Johnston, W., Mudumbai, S., Hoo, G., Jackson, K., Essiari, A. "Certificate-based Access Control for Widely Distributed Resources", Proceedings of the Eight Usenix Security Symposium, Aug, 1999
15. Thompson, M., Engert, D., Tuecke, S., " Internet X.509 Public Key Infrastructure Restricted Delegation Certificate Profile", draft-ggf-x509-res-delegation-01.txt , http://www.gridforum.org/security/ggf1_2001-03/draft-ggf-x509-res-delegation-01.pdf
16. Tuecke, S., Engert, D., Thompson, M., "Internet X.509 Public Key Infrastructure Impersonation Certificate Profile", draft-ggf-x509-impersonation-06.txt, http://www.gridforum.org/security/ggf1_2001-03/draft-ggf-x509-impersonation-06.pdf